AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (canceled)

2. (previously presented) A method according to claim 23, wherein said address token is transmitted in a cookie to said client application.

3. (previously presented) A method according to claim 23, wherein said address token is received from said client application with said authentication data.

4. (previously presented) A method according to claim 3, wherein a new address token is issued to said client application if said authentication data is invalid.

5. (previously presented) A method according to claim 4, wherein said address token comprises data indicating the number of times an invalid authenticator has been received from said client application.

6. (previously presented) A method according to claim 5, wherein said method comprises transmitting no further address token to said client application if an

address token received from said client application indicates that a predetermined number of invalid authenticators have been received from said client application.

7. (previously presented) A method according to claim 23, comprising timing out said address token of an application of a currently authenticated user if no document request is received from said client application for a predetermined period.

8. (previously presented) A method according to claim 23, comprising authenticating said user for access to a plurality of Web servers located in the same Internet domain; and

enabling each of said Web servers to validate document requests from the client application, which requests include said address token, by checking said status data on receipt of a document request.

9.-22. (canceled)

23. (currently amended) A method of operating an authenticating server system for authenticating a user of a client application provided on a client terminal having no unique IP address via a data communications network, the server system being arranged to control access to a document stored on a resource server connected to said data communications network, said method comprising performing the following steps in said server system:

receiving at the resource server a request for said document generated by said client application;

evaluating at the resource server client-side persistent information accompanying said request including checking if the client-side persistent information contains an address token previously issued by the resource server which uniquely identifies the user, and performing the following steps at the resource server:

i) if no address token which uniquely identifies the user is contained in the client-side persistent information accompanying said request:

generating an address token which uniquely identifies the user, the generated address token replacing an IP address of the client terminal as a way of identifying the user;

transmitting the generated address token to the client application in a client-side persistent information packet so that an address token which uniquely identifies the user is generated and transmitted without prior receipt at the resource server of a previously issued address token which uniquely identifies the user; and

storing said address token for the user; or

ii) if an address token which uniquely re-identifies the user is contained in the client-side persistent information accompanying said request and the address token is an unvalidated address token:

validating the address token using other authentication data received from the client terminal in said client-side persistent information and by reference to user authentication data already stored on said resource server;

storing the validated address token for an authenticated user and an access status of the authenticated user associated with the validated address token;

transmitting a client-side persistent information packet containing the validated address token to the client terminal;or

iii) if an address token which uniquely identifies the user is contained in the client-side persistent information accompanying said request and the address token is a validated address token, using said validated address token to enable said resource server to validate said request for said document by checking if said stored access status for said user includes access to said document.

24. (currently amended) A method as claimed in claim 23, wherein step (ii) further comprises:

transmitting said requested document to said client terminal along with ~~a~~ the client-side persistent information packet containing the validated address token to the client terminal.

25. (new) A method of operating an authenticating server system connected to a data communications network, the server system being arranged to authenticate a user of a client terminal connected via the data communications network to a resource server to control access by the user to a document stored on said resource server, the client terminal having no unique IP address, said method comprising:

storing within the authenticating server system authentication details of authorized users of said resource server;

authenticating the user by performing:

receiving authentication data and an unvalidated identifying tag at the resource server for the user from the client terminal,

validating said authentication data by determining if said authentication data corresponds to equivalent stored authentication details, and if so:

issuing a validated identifying tag for the user to said client terminal for storage thereon;

transmitting the validated identifying tag to the client terminal, the validated identifying tag being arranged to enable the client terminal to retransmit the validated identifying tag with document requests directed at said resource server; and

storing at the resource server status data indicating said validated identifying tag as identifying a terminal of a currently authenticated user; and

checking at the resource server said status data on receipt of a request for a document received from the client terminal, wherein if said resource server determines the request contains a validated identifying tag, the authenticated user is given access to the system.

26. (new) The method as in claim 25, wherein said validated identifying tag is transmitted in a cookie to said client terminal.

27. (new) The method as in claim 25, wherein in authenticating the user, said validated identifying tag is received from said client terminal with said authentication data.

28. (new) The method as in claim 27, wherein in authenticating the user, a new identifying tag is issued to said client terminal if said authentication data is invalid.

29. (new) The method as in claim 28, wherein said new identifying tag comprises data indicating the number of times an invalid authenticator and/or invalid authentication data have been received from said client terminal.

30. (new) The method as in claim 29, wherein said method further comprises issuing no further identifying tag to said client terminal if an identifying tag received from said client terminal indicates that a predetermined number of invalid identifying tags and/or invalid authentication data have been received from said client terminal.

31. (new) The method as in claim 25, comprising timing out said validated identifying tag as an identifying tag of a client terminal of a currently authenticated user if no document request is received from said client terminal for a predetermined period.

32. (new) The method as in claim 25, comprising authenticating said user for access to a plurality of Web servers located in a same Internet domain; and

enabling each of said Web servers to validate document requests from the client terminal, which requests include said validated identifying tag, by checking said status data on receipt of a document request.

33. (new) The method as in claim 25, wherein in said server system a plurality of documents are stored on a plurality of resource servers, wherein the step of validating the authentication data of a user comprises remotely authenticating the user by reference to authentication details of an authorized user stored by one of said plurality of resource servers, the remote authentication comprising:

generating status data to distinguish said user from other users who are not currently authenticated; and

generating a secret encryption key shared with said user, and wherein said method of operating the authentication server further comprises:

storing said status data in a storage device accessible to each of said plurality of resource servers to check an authentication status of said user by using said validated identifying tag for said client terminal received in said request; and

storing said shared secret key in a data store accessible by at least one of said resource servers for use during communications with said user.

34. (new) The method as in claim 33, wherein said authenticating step comprises issuing a challenge to the client terminal, receiving a response to said challenge, and verifying said response.

35. (new) The method as in claim 33, further comprising updating said status data for an authenticated user following said storing step in said storage device.

36. (new) The method as in claim 35, wherein said updating step is performed in response to a time-out associated with said status data.

37. (new) The method as in claim 35, wherein said updating step is performed in response to access by one of said resource servers to said status data.

38. (new) The method as in claim 36, wherein said updating step is performed in response to a request by the client terminal.

39. (new) The method as in claim 33, wherein said identifying tag is an IP address of the client terminal.

40. (new) The method as in claim 33, wherein said status data is stored in a data store which each of said resource servers are able to access.

41. (new) The method as in claim 33, wherein said authentication details include data identifying the rights of access of individual users to one or more of said resource servers.

42. (new) An authenticating server system adapted to perform the method of claim 25, wherein the client terminal supports a client application which the user uses to seek access to said document, and wherein the validated identifying tag comprises a unique identifying tag for the client application of the client terminal.

43. (new) An authenticating server system adapted to perform the method of claim 25.